(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平11－7241

(43)公開日　平成11年(1999)１月12日

(51)Int.Cl.[6]		識別記号	FI		
G09C	5/00		G09C	5/00	
G06F	12/14	310	G06F	12/14	310Z
G09C	1/00	660	G09C	1/00	660G
H04N	7/08		H04N	7/08	Z
	7/081				

審査請求　未請求　請求項の数10　ＦＤ　（全 13 頁）

(21)出願番号　特願平9－173168

(22)出願日　平成９年(1997)６月13日

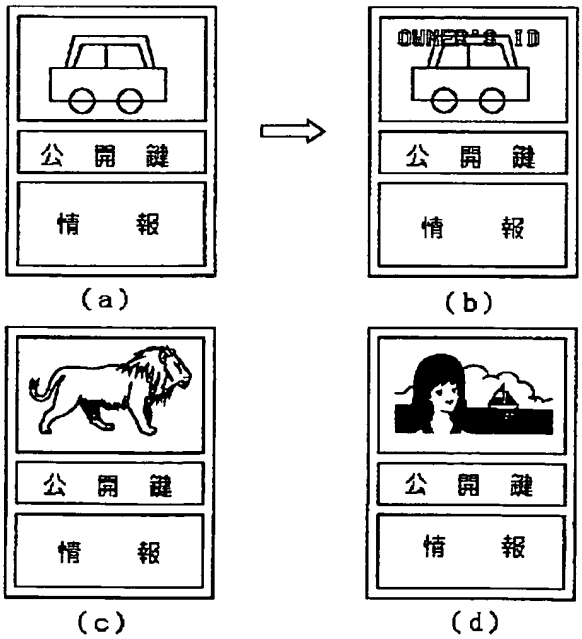
(71)出願人　000005979
三菱商事株式会社
東京都千代田区丸の内２丁目６番３号
(72)発明者　斉藤　誠
東京都千代田区丸の内二丁目６番３号　三菱商事株式会社内
(74)代理人　弁理士　南條　眞一郎

(54)【発明の名称】　電子透かしを利用するデジタルコンテンツ管理システム

(57)【要約】

【課題】　デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの管理を行うシステム及びデジタルコンテンツの管理に使用される公開鍵を配送するシステムを提供する。

【解決手段】　デジタルコンテンツ管理プログラムをマイクロカーネルとしてユーザ装置のオペレーティングシステムに組み込み、ネットワークあるいはデータ放送を利用して、デジタルコンテンツ管理プログラムとリンクする監視プログラムあるいは監視コマンドをユーザ装置に送信し、デジタルコンテンツの不正利用を監視する。不正利用されたデジタルコンテンツには可視透かしが埋め込まれ、以後の利用を抑制する。なお、正規の利用であっても不可視の透かしを埋め込むことにより複写・転送等の経路を確認することが可能になる。また、公開鍵を公開鍵配布画面に記入してネットワークあるいは放送により配布する。公開鍵配布画面には公開鍵所有者あるいは利用者の情報が不可視電子透かしとして埋め込まれたイメージ情報が添付されており、この電子透かしにより公開鍵あるいは利用者の正当性を確認する。



【特許請求の範囲】

【請求項１】　著作権主張がなされたデジタルコンテンツの管理を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
デジタルコンテンツ管理プログラムがユーザの装置のオペレーティングシステム中にマイクロカーネルとして組み込まれており；前記デジタルコンテンツ管理プログラムとリンクする利用監視プログラムが放送によって前記ユーザ装置に転送され；前記デジタルコンテンツ管理プログラムよりも割り込み優先度の高いプロセスとして前記利用監視プログラムが前記デジタルコンテンツの利用状況を監視する。

【請求項２】　前記利用状況として不正利用が検知された場合に前記デジタルコンテンツに前記ユーザの情報を可視透かしとして埋め込む、請求項１記載のデジタルコンテンツ管理システム。

【請求項３】　前記利用状況として不正利用が検知された場合に前記デジタルコンテンツに前記ユーザの情報を不可視透かしとして埋め込む、請求項１記載のデジタルコンテンツ管理システム。

【請求項４】　前記利用状況として保存・複写及び／又は転送がが検知された場合に前記デジタルコンテンツに前記ユーザの情報を不可視透かしとして埋め込む、請求項１記載のデジタルコンテンツ管理システム。

【請求項５】　公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
前記公開鍵が公開鍵配布画面に記入されて放送によって配布され；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記公開鍵の所有者の情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離して使用し；前記ユーザが前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより公開鍵所有者を確認する。

【請求項６】　前記公開鍵の所有者の情報として前記公開鍵の所有者の情報の電子指紋が利用される、請求項５記載のデジタルコンテンツ管理システム。

【請求項７】　公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
前記ユーザが前記公開鍵管理センタに前記公開鍵の配布を要求し；前記公開鍵管理センタが前記公開鍵を公開鍵配布画面に記入して前記ユーザに配布し；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記公開鍵の所有者の情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離して使用し；前記ユーザが前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより前記公開鍵の所有者を確認する。

【請求項８】　前記公開鍵の所有者の情報に代えて、前記公開鍵の所有者の情報の電子指紋が利用される、請求項７記載のデジタルコンテンツ管理システム。

【請求項９】　公開鍵管理センタがユーザに対して公開鍵の配送を行うデジタルコンテンツ管理システムであって：前記デジタルコンテンツ管理システムは、
前記ユーザが前記公開鍵管理センタに前記ユーザの情報を提示して前記公開鍵の配布を要求し；前記公開鍵管理センタが前記公開鍵を公開鍵配布画面に記入して前記ユーザに配布し；前記公開鍵配布画面にはイメージ情報が添付され；前記イメージ情報には前記ユーザの情報が不可視電子透かしとして埋め込まれ；前記ユーザが前記公開鍵配布画面から前記公開鍵を分離し、前記公開鍵を用いて暗号化されたデジタルコンテンツとともに前記公開鍵配布画面を前記公開鍵の所有者に転送し；前記公開鍵の所有者が前記公開鍵管理センタに前記公開鍵配布画面を提示すると前記公開鍵管理センタが前記不可視電子透かしにより前記ユーザを確認する。

【請求項１０】　前記ユーザに代えて、前記ユーザの情報の電子指紋が利用される、請求項９記載のデジタルコンテンツ管理システム。

【発明の詳細な説明】

【０００１】

【利用分野】本発明は、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの著作権管理、デジタルコンテンツの秘密保護、を行うシステムに関する。

【０００２】

【従来の技術】情報化時代と呼ばれる今日、これまでは各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつある。このデータベースシステムにおいてこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム２値データであり、自然画及び動画のような情報量が格段に多いデータを取扱うことができなかった。

【０００３】ところで、各種電気信号のデジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた２値データ以外の画像信号もデジタル処理技術の開発が進められている。この画像信号のデジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をデジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【０００４】従来広く普及しているアナログコンテンツは保存，複写，加工，転送をする毎に品質が劣化するた

めに、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルコンテンツは保存，複写，加工，転送を繰り返して行っても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルコンテンツの著作権処理には的確な方法がなく、著作権法であるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【０００５】データベースの利用法は単にその内容を参照するだけでなく、通常は得たデジタルコンテンツを保存，複写，加工することによって有効活用し、加工したデジタルコンテンツを通信回線を経由してオンラインであるいは適当な記憶媒体を利用してオフラインで他人に転送したりさらにはデータベースに対して転送し、新しいデータとして登録することさえ可能である。従来のデータベースシステムにおいては文字データのみが対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログコンテンツである音声データ及び画像データがデジタルコンテンツ化されてデータベースとされる。

【０００６】このような状況において、データベース化されたデジタルコンテンツの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写，加工，転送等の２次利用について完成された著作権管理手段はない。なお、広告付きソフトあるいはフリーウェアと呼ばれるデジタルコンテンツは利用において原則として使用料を必要としないが、著作権は存在しており、利用の仕方によっては著作権上の制限を受ける場合がある。

【０００７】このような状況に鑑みて、本発明者はこれまでにデジタルコンテンツの著作権を保護することを目的としてこれまでに様々な提案を行ってきた。本発明者らは特開平６－４６４１９号及び特開平６－１４１００４号で公衆電信電話回線を通じて鍵管理センタから許可鍵を入手することによって著作権管理を行うシステムを、特開平６－１３２９１６号でそのための装置を提案した。

【０００８】また、特開平７－２７１８６５号及び特開平８－１８５４４８号において、デジタルコンテンツの著作権を管理するシステムについて提案した。これらのシステム及び装置において、暗号化された番組の視聴を希望する者は通信装置を使用し通信回線を経由して管理センタに視聴申し込みを行い、管理センタはこの視聴申し込みに対して許可鍵を送信するとともに課金処理を行い料金を徴収する。許可鍵を受信した視聴希望者はオンラインあるいはオフライン手段によって許可鍵を受信装置に送り込み、許可鍵を送り込まれた受信装置はその許可鍵によって暗号化された番組の暗号を解除する。

【０００９】特開平７－２７１８６５号に記載されたシステムは、デジタル映像コンテンツのリアルタイム送信も含むデータベースシステムにおけるデジタルコンテンツの表示（音声化を含む），保存，複写，加工，転送における著作権の管理を行うために、利用を許可する鍵の他に、著作権を管理するためのプログラム及び著作権情報を用いる。この著作権管理プログラムは、申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【００１０】また、この特開平７－２７１８６５号には、デジタルコンテンツが暗号化された状態でデータベースから供給され、著作権管理プログラムによって表示・加工のときにのみ復号化され、保存，コピー，転送は再び暗号化された状態で行うことが記載されている。さらに、著作権管理プログラム自体を暗号化し、許可鍵で著作権管理プログラムを復号化し、復号化された著作権管理プログラムが著作権データの復号化及び暗号化を行うこと、データの保存及び表示以外の利用が行われた場合には操作者についての情報を含む著作権情報を原著作権情報に加えて履歴として保存することも記載されている。

【００１１】本出願が関連する特開平８－２８７０１４号において著作権管理を行うためのボード，ＰＣＭＣＩＡカードあるいはＩＣカードの形態を有する復号／再暗号化用装置及び暗号鍵の寄託システムを提案した。またこの出願では著作権管理方法のテレビジョン会議及び電子商取引への応用についても言及した。

【００１２】特開平８－２７２７４５号において複数データを利用した加工データの原データ著作権及び加工データ著作権の保護を秘密鍵方式と公開鍵方式を組み合わせて加工プログラムへのデジタル署名で申込みの正当性を確認することによって行うシステムを提案した。

【００１３】特開平８－２８８９４０号において、データベース，ビデオオンデマンド（ＶＯＤ）システムあるいは電子商取引に著作権管理システムを適用するための様々の形態を提案した。

【００１４】特開平８－３２９０１１号において、複数データを利用・加工する場合の原データ及び新データの著作権保護を第三の暗号鍵及び著作権ラベルを用いて行うシステムを提案した。

【００１５】以上説明した本発明者が提案してきたデータ著作権管理システム及びデータ著作権管理装置から理解されるように、データ著作権の管理は著作権管理プログラムによって暗号化／復号化／再暗号化及び利用内容の制限を行うことによって実現される。この暗号技術及び利用制限はコンピュータを使用することによって実現される。

【００１６】さらに、ネットワークを経由して秘密情報を交換する場合には窃取防止のために情報の暗号化が行われる。伝送時の情報窃取を暗号化により防止すること

が、ＵＳＰ５５０４８１８，５５１５４４１に述べられており、その場合に複数の暗号鍵を用いることがＵＳＰ５５０４８１６，５３５３３５１，５４７５７５７及び５３８１４８０に述べられており、再暗号化を行うことがＵＳＰ５４７９５１４に述べられている。

【００１７】コンピュータを効率的に使用するために、コンピュータの全体の動作を統括するオペレーティングシステム（ＯＳ）が用いられている。パーソナルコンピュータ等で使用されている従来のオペレーティングシステムはメモリ管理，タスク管理，割り込み，プロセス間通信という基本的なサービスを扱うカーネル（Kernel）と、その他のサービスを扱うオペレーティングシステムサービスで構成されていた。

【００１８】しかしながら、マイクロプロセッサの能力向上、主記憶装置として使用されるＲＡＭ価格の低下というコンピュータ側の情勢変化と、コンピュータに対する利用者からの要求性能の向上に伴い、コンピュータの全体の動作を統括するオペレーティングシステムも機能向上が要求され、以前と比較してオペレーティングシステムの規模が肥大している。

【００１９】このような肥大したオペレーティングシステムはオペレーティングシステム自身がその保存場所であるハードディスクの大きなスペースを占領するため、ユーザが必要とするアプリケーションプログラムあるいはデータを保存するスペースが不足がちになり、コンピュータの使い勝手が悪くなるという事態が発生する。

【００２０】このような事態に対処するために、最新のオペレーティングシステムはカーネルから他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステムと、セキュリティサブシステム等の中枢サブシステムとをユーザに依存する部分であるサブシステム(Sub system)として取り除き、ハードウェアの相異を吸収するＨＡＬ(Hardware abstraction Layer)，スケジューリング機能，割り込み機能，Ｉ／Ｏ管理機能等の基本的部分をマイクロカーネル(Micro kernel)とし、サブシステムとマイクロカーネルの間にシステムサービスＡＰＩ(Application Programming Interface)を介在させてオペレーティングシステムを構成している。

【００２１】このようにすることにより、機能変更あるいは追加によるオペレーティングシステムの拡張性が向上するとともに、用途に対応する移植が容易になる。また、マイクロカーネルの要素をネットワーク化された複数のコンピュータに分散配置することにより、分散オペレーティングシステムを実現することが容易になる。

【００２２】コンピュータはデスクトップ型あるいはノート型に代表されるパーソナルコンピュータ以外に、コンピュータ周辺機器、各種制御装置、通信機等に使用されている。その場合、各々の装置に適合するエンベッデッド（組み込み）用の専用オペレーティングシステムとしてマン・マシン・インターフェースが重視される汎用のパーソナルコンピュータ用オペレーティングシステムと異なり、実行の早さが重視されるリアルタイムオペレーティングシステムが採用されている。

【００２３】当然のこととして組み込まれる装置毎に異なる専用のオペレーティングシステムの開発費用は大きい。　そのため、最近ではエンベデッド（組み込み）用のリアルタイムオペレーティングシステムとしてパーソナルコンピュータ用の汎用オペレーティングシステムを転用することが提案されており、マイクロカーネルと組み合わされるサブシステムにエンベデッド用の固有のプログラムを配置することにより、組み込み用のリアルタイムオペレーティングシステムを得ることが行われている。

【００２４】オペレーティングシステムの大きな機能としてスケジューリングや割り込み処理等のタスク管理がある。タスク管理に関して、オペレーティングシステムには大きく分けて同時に１つのタスク処理しか行わないシングルタスク方式と、同時に複数のタスク処理を行うマルチタスク方式があり、マルチタスク方式はさらにタスクの切り替えが処理されるタスクに依存するマルチタスク方式と、処理されるタスクに依存しないマルチタスク方式に区分される。

【００２５】これらの中、シングルタスク方式はＭＰＵに１つのプロセスを割り当てそのプロセスが終了するまでＭＰＵを解放しないものであり、ノンプリエンプティブマルチタスク方式はＭＰＵを時分割して複数のプロセスに割り当てることができるが、実行中のプロセスがオペレーティングシステムに制御を戻さない限り他のプロセスは実行されないものであり、プリエンプティブマルチタスク方式はある時間間隔で実行中のプロセスに割り込みを行い、他のプロセスに強制的に制御を移すものである。したがって、リアルタイムのマルチタスクはプリエンプティブ方式の場合にのみ可能である。

【００２６】コンピュータにおけるタスク管理はメモリやファイルなどのシステム資源を持つ単位であるプロセスに基づいて行われ、プロセスの管理はプロセスを細分化したＣＰＵ時間を割り当てる単位であるスレッドに基づいて行われる。なお、この場合システム資源は同一プロセス内の全てのスレッドで共有され、したがって一つのプロセス中にはシステム資源を共有する一つ以上のスレッドが存在することになる。

【００２７】マルチタスク方式で処理される各タスクには優先順位(Priority Spectrum)があり、一般的には３２の段階に分けられる。この場合、割り込みを行わない通常のタスクは０－１５段階に分けられるダイナミッククラス(Dynamic Classes)に区分され、割り込みを行うタスクは１６－３１段階に分けられるリアルタイムクラス(Real-Time Classes)に区分される。割り込み処理はタイムスライスと呼ばれる割り込み可能時間（通常１０ms）を単位として行われ通常の割り込みは１０msのタイ

ムスライスで行われている。このような状況において、最近リアルタイムスライスと呼ばれる割り込み可能時間が１００μsであるタイムスライスが提案されたが、このリアルタイムスライスを利用すれば従来の１０msの割り込みよりも優先して割り込みが可能である。

【００２８】暗号技術はデータコンテンツの不正利用を不可能にするための手段であるが、その動作が完璧であるとの保証はないため、不正利用の可能性を完全に否定することができない。一方、電子透かし技術は不正利用を不可能にすることはできないが、不正利用が発見されたときには、電子透かしの内容を検証することにより不正利用であることを確定することができるが手段であり、種々の方法があるが日経エレクトロニクス６８３号，ｐ.９９～１２４に「「電子透かし」がマルチメディア時代を守る」（１９９７／２／２４，日経ＢＰ社刊）に全般的に紹介されており、また同号，ｐ.１４９～１６２,ウォルター・ベンダー他「電子透かしを支えるデータ・ハイディング技術（上）」及び６８４号,ｐ.１５５～１６８,「電子透かしを支えるデータ・ハイディング技術（下）」(IBM System Journal, vol.35, nos.3 & 4(International Business Machines Corporation)から転載）にも紹介されている。この電子透かし技術については、ＥＰ６４９０７４にも述べられている。

【００２９】

【発明の概要】本件出願においては、デジタルコンテンツの管理、特に著作権主張がされたデジタルコンテンツの管理を行うシステム及びデジタルコンテンツの管理に使用される公開鍵を配送するシステムを提案する。

【００３０】本出願で提案するデジタルコンテンツ管理システムでは、ネットワークあるいはデータ放送を利用して著作権主張がされたデジタルコンテンツの不正利用を監視する。デジタルコンテンツ管理プログラムをマイクロカーネルとしてユーザ装置のオペレーティングシステムに組み込み、著作権主張がされたデジタルコンテンツの利用はこのデジタルコンテンツ管理プログラムによって管理される。

【００３１】ユーザ装置は、利用監視プログラムとリンクするデジタルコンテンツ管理プログラムの管理下に置かれ、利用監視プログラムはデジタルコンテンツ管理プログラムよりも割り込み優先度の高いプロセスとして動作する。この利用監視プログラムは著作権主張がされたデジタルコンテンツの不正利用を監視し、不正利用が行われている場合には、利用の停止、警告あるいはデジタルコンテンツへの可視電子透かしの埋め込みを行う。また、正規利用の場合にも利用状況の追跡を行うために可視電子透かしに代えて不可視電子透かしを埋め込むことができる。

【００３２】さらに、本出願では公開鍵をネットワークあるいは放送により配布するシステムを提案する。公開鍵は公開鍵配布画面に記入されて配布されるが、公開鍵配布画面には公開鍵所有者の情報が不可視電子透かしとして埋め込まれたイメージ情報が添付されている。利用者が公開鍵配布画面を公開鍵管理センタに提示すると公開鍵管理センタが不可視電子透かしにより公開鍵所有者の正当性を確認する。

【００３３】公開鍵をネットワークにより配布する場合には、公開鍵所有者の情報あるいは公開鍵を請求したユーザの情報を不可視電子透かしとして埋め込み、埋め込まれた不可視電子透かしを確認することにより、公開鍵の正当性あるいはユーザの正当性を確認することができる。その場合、ユーザの情報としてユーザの公開鍵の電子指紋を利用すれば、確認が容易になる。

【００３４】

【実施例】図面を用いて本願発明の実施例を説明する。デジタルコンテンツの著作権保護においてはユーザ側装置での不正利用を如何に防止するかが最大の課題であり、特開平７－２７１８６５号の「データベース著作権管理方法」ではこれを目的としてデジタルコンテンツ管理プログラムにより復号／再暗号及び利用制限が行われる。しかしながら、著作権保護の対象であるデジタルコンテンツはユーザ側装置によって復号／再暗号が行われるため、復号／再暗号の処理及びそのために使用される暗号鍵の管理が万全であることは期しがたく、デジタルコンテンツ管理プログラムを無効化することによりデジタルコンテンツが不正に保存・複写・転送・加工される可能性がある。

【００３５】このような不正利用を制限するためには、デジタルコンテンツの復号／再暗号処理及び暗号鍵の管理を行うデジタルコンテンツ管理プログラムがユーザによって改変されないようにする必要があり、そのためにはデジタルコンテンツ管理プログラムのハードウェア（ファームウェア）化が最も確実な方法である。例えば、現在アナログテレビジョン放送においてスクランブルされた放送番組のデスクランブルに使用されている専用のスクランブルデコーダのような専用のデジタルコンテンツ管理装置を使用することによってのみデジタルコンテンツの復号／再暗号処理及び暗号鍵の管理が可能なようにする構成がある。

【００３６】このような構成は確実ではあるがシステム構成が柔軟性に欠けており、ユーザ側装置の変更あるいはデジタルコンテンツ管理プログラムの変更が行われた場合に、ユーザがこれらの変更に対応することは大変である。

【００３７】ユーザ側装置の変更あるいはデジタルコンテンツ管理プログラムの変更が行われた場合であっても、柔軟に対処するためにはデジタルコンテンツ管理プログラムがソフトウェアであることが望ましいが、デジタルコンテンツ管理プログラムがアプリケーションプログラムである場合には改変が行われる可能性がある。したがって、デジタルコンテンツ管理プログラムがソフト

ウェアであるためには、ユーザが改変を行うことができないオペレーティングシステム（ＯＳ）の固定領域であるカーネルにデジタルコンテンツ管理プログラムを組み込む必要がある。

【００３８】しかし、カーネルという固定領域にデジタルコンテンツ管理プログラムを組み込んだ場合には、データベースによってデジタルコンテンツ管理システム及び暗号システムが異なっているような場合に現実的ではない。

【００３９】前に述べたように、リアルタイムオペレーティングシステムにはカーネル領域も含む他のオペレーティングシステム内のシステムのタイムスライス時間よりも１～２桁早いリアルタイムスライス時間で割り込み動作可能なものがあり、この技術を利用することにより、全体の動作に影響を与えることなく著作権主張のあるデジタルコンテンツの利用状況を監視し、不正利用が発見された場合には、警告あるいは利用の強制中止をすることができる。次にリアルタイムオペレーティングシステムを利用してデジタルコンテンツ管理プログラムを補強する方法を説明する。

【００４０】デジタルコンテンツの不正利用は復号されたデジタルコンテンツの無許可加工、無許可保存、無許可複写あるいは無許可転送することによって行われるから、不正利用の有無は復号化デジタルコンテンツの加工、保存、複写あるいは転送の有無によって検出することができる。そのために、不正利用を監視するプロセスは、ある時間間隔でデジタルコンテンツ管理プログラムが実行中のプロセスに割り込みを行い、強制的に監視を行うプリエンプティブ方式のマルチタスクにより割り込みを行う。

【００４１】通常使用されるマルチタスクタイムスライスは１０ｍｓであり、復号／再暗号プロセスもこの時間単位で行われる。一方、最速のリアルタイムスライスは１／１００の１００μｓである。したがって、復号されたデジタルコンテンツが加工、保存、複写あるいはアップロードされているか否かを割り込み優先順位の高い監視タスクにより監視することにより、ユーザが行っている正当な利用に影響を与えることなく著作権主張のあるデジタルコンテンツの利用状況を監視することができ、不正利用が発見された場合には、警告あるいは利用の強制中止をすることができる。

【００４２】このような監視機能を有するデジタルコンテンツ管理プログラムはオペレーティングシステムのカーネル部分ではなくユーザモードで動作するサブシステム領域に組み込み、監視プロセスは優先順位の高いプロセスとする。

【００４３】この構成により、復号／再暗号によるデジタルコンテンツの利用と許可外の不正利用の有無の監視を同時に、かつ円滑に実行することができる。

【００４４】図１に、デジタルコンテンツ管理プログラムが組み込まれたオペレーティングシステムの構成を示す。このオペレーティングシステムはユーザが操作することができないカーネルモードで動作する管理部(Executive)と、ユーザが操作することができるユーザモードで動作するサブシステムからなり、管理部とサブシステムとはシステムサービスＡＰＩ(Application Programming Interface)によってインターフェースされており、ハードウェアとカーネル部の間にはＨＡＬ(Hardware abstraction Layer)が介在している。

【００４５】サブシステムは、他のオペレーティングシステムのエミュレーション及び画面描画を行う環境サブシステム及びセキュリティサブシステム等の中枢サブシステムとアプリケーションプログラムから構成されている。

【００４６】管理部には、マイクロカーネル(micro kernel)である仮想記憶管理機能(virtual memory manager)、オブジェクトマネージャ、ＬＰＣ(Local Procedure Call)機能、プロセスマネージャ、セキュリティ参照モニタと、最も基本的な要素であるカーネルとディスク及びネットワークとの間の入出力を管理するＩ／Ｏ管理機能(I/O manager)に、さらに著作権主張がされたデジタルコンテンツの管理を行うデジタルコンテンツ管理プログラム、すなわちデジタルコンテンツ管理機能(digital content manager)が組み込まれており、デジタルコンテンツの管理における重要な部分である保存、複写あるいは転送の管理はデジタルコンテンツ管理機能がＩ／Ｏ管理機能を管理することによって行われる。

【００４７】図２に示されたのは、本願発明が適用されるデジタルコンテンツ管理システムの実施例である。このデジタルコンテンツ管理システムにおいて、ユーザによるデジタルコンテンツ利用状況の監視はネットワークを介して行われる。この図において、１はデータベース、２はデジタルコンテンツ管理センタ、４はユーザであり、ユーザ４とデータベース１及びデジタルコンテンツ管理センタ２は公衆通信回線あるいは双方向性ＣＡＴＶ回線であるネットワーク３で接続されている。

【００４８】データベース１にはデジタルコンテンツが蓄積されており、破線で示された経路５を経由して暗号化デジタルコンテンツがユーザ４に転送される。データベース１は暗号化デジタルコンテンツを復号／再暗号するための復号用暗号鍵及び再暗号用暗号鍵を経路６によりデジタルコンテンツ管理センタ２に転送し、デジタルコンテンツ管理センタ２は転送された復号用暗号鍵及び再暗号用暗号鍵を暗号化し、破線７で示された経路を経由してユーザ４に配送する。また、デジタルコンテンツ管理センタ２は監視プログラムを実線で示された経路８でユーザ４に送信する。

【００４９】利用許可内容はユーザ４が使用する装置に組み込まれているデジタルコンテンツ管理プログラムによって管理されているが、悪意のあるユーザによってデ

ジタルコンテンツ管理プログラムが管理している範囲外の利用が行われる可能性を完全には否定することができない。デジタルコンテンツ管理プログラムはユーザ４の装置の入出力を管理しており、ユーザにおけるメモリからの入出力すなわち保存・複写・転送はすべてデジタルコンテンツ管理プログラムによって管理されており、デジタルコンテンツが保存・複写・転送されるときには再暗号化される。しかし、悪意のあるユーザによって、万一、この管理ができないようにされた場合でもデジタルコンテンツの保存・複写・転送が行われていることはデジタルコンテンツ管理プログラムに割り込む監視プログラムによって検知される。

【００５０】監視プログラムはユーザ４が使用する装置に組み込まれているデジタルコンテンツ管理プログラムとリンクしてデジタルコンテンツ管理プログラムの処理に割り込むことにより監視動作を行い、ユーザが利用許可内容を越えた利用を行なっているかどうかを監視し、このような不正規の利用である保存・複写・転送が行われていることを検知した監視プログラムは特開平７－２７１８６５号に示された警告の表示に代えて、復号処理の停止，ユーザが関知しない暗号鍵による強制再暗号化あるいは図３（ａ）に示された原デジタルコンテンツへの図３（ｂ）に示された可視電子透かしの埋め込み、あるいは図４（ｂ）に示された不可視電子透かしのデジタルコンテンツへの埋め込みを行う。

【００５１】ここで利用許可内容というのは、デジタルコンテンツの，単純利用，内蔵記憶装置への保存，外部媒体への複写，ネットワークを経由しての他の利用者への転送を指す。なお、可視電子透かしとして埋め込まれるのはユーザの名前等識別容易なものが適切である。

【００５２】ユーザ装置に内蔵されているデジタルコンテンツ管理プログラムの動作中は監視プログラムが協働している。言い換えれば、監視プログラムと協働していなければデジタルコンテンツ管理プログラムが動作しないようにされている。そのためには、ネットワークを経由して監視プログラムが起動していることをデジタルコンテンツ管理プログラムを起動させるための条件にするか、あるいはデジタルコンテンツ管理プログラムを起動させると自動的にネットワークを経由して監視プログラムが起動されるようにされている。ユーザがネットワーク経由でユーザに転送されるデジタルコンテンツを利用する場合には、転送されるデジタルコンテンツに混入して監視プログラムも転送される。

【００５３】なお、監視プログラムをデジタルコンテンツ管理プログラムに一体化し、デジタルコンテンツ管理プログラムに監視動作を行わせる監視コマンドを送信してデジタルコンテンツ管理プログラムに監視動作を行わせるようにすることもできる。

【００５４】ネットワークを介して行うデジタルコンテンツ管理システムにおいて、画像データ等情報量の多いデジタルコンテンツを扱う場合には、通信回線としてＩＳＤＮ(Integrated System for Digital Network)回線を使用することが多い。このＩＳＤＮ回線として一般的に使用されているものは、Ｂチャンネルと呼ばれるデータ伝送速度が６４Kbpsであるデータチャンネルが２チャンネル、Ｄチャンネルと呼ばれるデータ伝送速度が１６Kbpsである制御チャンネルが１チャンネルあり、当然のこととしてデジタルコンテンツは１～２チャンネルのデータチャンネルで伝送されるが、Ｄチャンネルは使用されていないことが多い。そこで、監視プログラムによる割り込み監視をこのＤチャンネルで行うことにようにすれば、デジタルコンテンツの使用に全く影響与えることなく、利用状況の遠隔監視を行うことが可能になる。

【００５５】また、公衆通信回線を使用する場合にはダウンロード用に最大５６Ｋｂｐｓのデータ伝送速度を実現することができるＡＤＳＬ(asymmetric digital subscriber line)技術を利用することにより、監視プログラムによる割り込み監視を効率的に行うことができる。

【００５６】図４に示すのは、利用許可内容に含まれている正規の保存・複写・転送の場合であっても電子透かしを埋め込む例である。この場合の電子透かしは、電子透かし検出手段によって（ｂ）のように検出される不可視電子透かしであって、電子透かし検出手段によらない場合は（ａ）に示されたように原デジタルコンテンツと一見代わりはない。なお、可視電子透かしの場合と同様に埋め込まれるのはユーザの名前等識別容易なものが適切である。

【００５７】このようにすることにより、初めは正規利用であっても後で不正利用が行われた場合に保存・複写・転送の経路を確認することができる。また、正規のものであっても保存・複写・転送が繰り返されることにより、（ｃ）に示されたように不可視電子透かしが増え、その結果デジタルコンテンツの品質が低下する。このようなことによって無限に保存・複写・転送が繰り返されることがなくなり、デジタルコンテンツの管理が容易になる。

【００５８】デジタルコンテンツ管理のために重要な要素である「再暗号化」はユーザの装置にとってかなり負担の重いプロセスである。そのため、簡易型として電子透かしを埋め込むだけでもデジタルコンテンツの不正利用を防止するには有効である。

【００５９】デジタルコンテンツの利用が有料で行われる場合に、特開平７－２７１８６５号に示されているようにユーザが予め利用許可鍵を入手するようにすれば、課金は容易に行われるが、デジタルコンテンツ管理センタが利用実績であるメータリングデータを後でポーリングによって回収して課金を行う場合には、ポーリングが行われるまでメータリングデータはユーザの管理下におかれる。そのため、悪意あるユーザによってメータリングデータの改竄が行われ、正常な課金が妨げられること

が考えられる。

【００６０】この実施例のデジタルコンテンツ管理システムにおいてはユーザがデジタルコンテンツを利用している時にはユーザ装置は常に管理センタに接続され、監視プログラムによる利用状況の監視が行われている。したがって、この監視動作の中でメータリングデータをデジタルコンテンツ管理センタに保管することにより、ポーリングの必要がなくなり、ユーザによるメータリングデータの改竄を防止することができる。また、デジタルコンテンツの利用が無料で行われる場合であっても、ユーザによる利用状況を容易に把握することができる。

【００６１】図５に示されたのは、本願発明が適用されるデジタルコンテンツ管理システムの他の実施例の構成図である。このデジタルコンテンツ管理システムにおいて、デジタルコンテンツ利用状況の監視は放送によって行われる。この図において、１１はデータベース、１２はデジタルコンテンツ管理センタ、１４はユーザであり、ユーザ１４とデータベース１及びデジタルコンテンツ管理センタ１２は公衆通信回線あるいは双方向性ＣＡＴＶ回線であるネットワーク１３で接続されている。

【００６２】データベース１１にはデジタルコンテンツが蓄積されており、破線で示された経路１５を経由して暗号化デジタルコンテンツがユーザ１４に転送される。デジタルコンテンツ管理センタ１２は暗号化デジタルコンテンツを復号／再暗号するための復号用暗号鍵及び再暗号用暗号鍵を暗号化し、破線１７で示された経路を経由してユーザ１４に配送する。また、デジタルコンテンツ管理センタ１２は監視コマンドを放送局１９に転送し、放送局１９は転送された監視コマンドを実線で示された経路１８でユーザ１４に送信する。

【００６３】この経路１８は放送電波が最も一般的であるが、有線放送であるＣＡＴＶケーブルも利用可能であり、さらにインターネット放送が行われている場合にはネットワークを利用することも可能である。

【００６４】この監視コマンドはユーザ１４が使用する装置に組み込まれているデジタルコンテンツ管理プログラムが行っている動作に割り込み、ユーザが利用許可内容を越えた利用を行なっているかどうかをデジタルコンテンツ管理プログラムに監視させ、保存・複写・転送が行われるときには復号処理を停止させ、あるいは図３に示された可視電子透かし又は図４に示された不可視電子透かしをデジタルコンテンツに埋め込む。

【００６５】ユーザ装置に内蔵されているデジタルコンテンツ管理プログラムの動作中は監視コマンドが割り込み動作を行っている。言い換えれば、監視コマンドが放送されている放送波を受信していなければデジタルコンテンツ管理プログラムが動作しないようにされている。そのためには、放送波を経由して監視コマンドを受信していることをデジタルコンテンツ管理プログラムを起動させるための条件にするか、あるいはデジタルコンテンツ管理プログラムを起動させると自動的に放送波を経由する監視コマンドを受信する。ユーザがデータ放送等でユーザに転送されるデジタルコンテンツを利用する場合には、転送されるデジタルコンテンツに混入して監視コマンドも転送される。

【００６６】デジタルコンテンツ管理プログラムはユーザ１４の装置の入出力を管理しており、ユーザにおけるメモリからの入出力すなわち保存・複写・転送はすべてデジタルコンテンツ管理プログラムによって管理され、デジタルコンテンツが保存・複写・転送されるときには再暗号化される。悪意のあるユーザによって、万一、この管理ができないようにされた場合でもデジタルコンテンツの保存・複写・転送が行われていることはデジタルコンテンツ管理プログラムに割り込む監視プログラムによって検知される。

【００６７】このような不正規の利用が行われていることを検知した監視プログラムは特開平７－２７１８６５号に示された警告の表示に代えて、図３（ｂ）に示されたような可視電子透かしの埋め込みを行う。また、利用許可内容に含まれている正規の保存・複写・転送の場合であっても図４（ｂ）及び（ｃ）に示されたような、電子透かし検出手段によってはじめて検出される不可視電子透かしを埋め込むことも可能である。

【００６８】これらの放送あるいはネットワークを介しての監視動作は、ユーザがユーザの意志で行うのではなく、著作権主張がされたデジタルコンテンツを利用する場合にはデジタルコンテンツ管理プログラムにより自動的に行われる。さらにこの動作を確実にするには、放送あるいはネットワークを介しての監視動作が行われていない場合にはデジタルコンテンツ管理プログラムによる復号／暗号化等の動作が行われないようにされる。また、著作権主張がされたデジタルコンテンツを利用する場合には監視プログラムを放送する電波の受信あるいは監視プログラムを送信する管理センタに自動的に接続される。

【００６９】次に、公開鍵の配布を行う実施例を説明する。共通鍵(common key)システムとも呼ばれる秘密鍵(secret key)システムで使用される暗号鍵の大きさは大きいものでも１００ビット程度であるのに対して、公開鍵(public key)システムで使用される暗号鍵は大きいものは１０００ビットを越す。公開鍵システムは安全性が高い反面暗号化／復号化に手間がかかるため、秘密鍵の送付、デジタル署名、認証等容量の小さいデータの暗号化に用いられ、デジタルコンテンツの暗号化は秘密鍵を用いて行われる。公開鍵システムでは公開鍵と専用鍵(private key)が組み合わされて使用され、専用鍵は所有者の管理下におかれ、他人が知ることはできないが、公開鍵はその使用目的上、他人に知らされている必要がある。

【００７０】そのために、公開鍵は種々の手段で公衆に

配布されるが、その際に所有者から直接に公開鍵を受領することができれば偽の公開鍵を配布される恐れは少ないが、そうでない場合には偽の公開鍵を受領してしまうことがある。この実施例では公開鍵を放送あるいはネットワークを経由するという間接的な配布方法においても配布された公開鍵の真偽を用にに確認することができるデジタルコンテンツ管理システム、いわば鍵配信ネットワークを提案する。

【００７１】図６に、放送により公開鍵の配布を行うデジタルコンテンツ管理システムの本発明の実施例を示す。このデジタルコンテンツ管理システムでは、公開鍵は広く一般に配送されるため、電子商取引等における公開鍵認証方式で採用されるＰＥＭ(Privacy Enhanced Mail)方式に代わる簡易認証方式として用いることができる。

【００７２】この図において、２１は公開鍵所有者、２２は公開鍵管理センタ、２３は放送局、２４はネットワーク、２５はユーザである。放送局２３は地上波アナログ、衛星アナログ、ＣＡＴＶアナログ、地上波デジタル、衛星デジタル、ＣＡＴＶデジタル等のテレビジョンあるいは音声放送局であり、走査線多重(Vertical Blanking Interval:VBI)、音声多重、データ混入等適宜の手段によりデータ放送が行われる。なお、この放送局としてインターネット放送局も利用可能である。ネットワーク２４は公衆通信回線あるいは双方向性ＣＡＴＶ回線であり、公開鍵管理センタ２２とユーザ２５との間はネットワーク２４で接続されており、放送局２３とユーザ２５との間は適宜な情報伝達媒体により接続される。

【００７３】このように構成されたデジタルコンテンツ管理システムにおいて、公開鍵所有者２１は所有する公開鍵と公開鍵所有者本人であることを証明する何らかのデータを公開鍵所有者識別用データとして経路２６により公開鍵管理センタ２２に転送する。ここで使用される公開鍵所有者識別用データとして、公開鍵所有者名等の情報を直接に利用されるが、その情報をＭＤ５ハッシュアルゴリズムによって１６バイトのデータに縮小した電子指紋を利用することもできる。

【００７４】公開鍵管理センタは図７（ａ）に示されたような公開鍵配布画面を用意しておき、所定の位置に公開鍵を挿入する。この画面は挿入された公開鍵を容易に分離して使用することができるようにＨＴＭＬ(Hyper Text Markup Language)形式あるいはＸＭＬ(eXtensible Markup Language)形式を使用して作成されており、その一部にはイメージデータが挿入されている。

【００７５】このイメージデータには、公開鍵所有者２１の識別用データ(OWNER'S ID) が不可視の電子透かしとして埋め込まれている。この不可視の電子透かしのアルゴリズム及び埋め込み位置は公開鍵管理センタのみが知っており、公開鍵管理センタは図７（ｂ）に示されたように電子透かしの内容を知ることができるが、その他の者が見た場合には図７（ａ）のような通常の画面であり、電子透かしの内容を知ることはできない。

【００７６】このイメージ画面として広告を掲載しておけば公開鍵配布に要する経費を広告掲載料によって賄うことができる。また、その他の部分には緊急情報・告知情報等の付加情報を掲載することができる。さらに、有効期間を設ける等の管理を行うためにタイムスタンプを付加してもよい。このイメージデータとしては写真を利用することが最適であるが、音声データが利用可能な場合には利用される音声データに電子透かしを埋め込むことも可能である。

【００７７】放送局２３は、このようにして作成された公開鍵配布画面を放送経路２８により放送する。

【００７８】放送された公開鍵配布画面をユーザ２５が受信するが、ユーザ２５が受信した公開鍵配布画面のイメージ画面に埋め込まれた電子透かしは不可視のものであるから、ユーザ２５は電子透かしの内容を知ることはできない。

【００７９】ユーザ２５は、放送された公開鍵配布画面から公開鍵を分離して各種電子商取引に使用するが、公開鍵の真偽に疑いを持った場合にはネットワーク２４による経路２９により公開鍵配布画面を公開鍵管理センタ２２に転送する。

【００８０】公開鍵管理センタ２２は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、図７（ｂ）に示されたように検出された公開鍵所有者の識別情報についてネットワーク２４による経路３０によりユーザ２５に通知する。

【００８１】このようにすることにより、他人が成りすましていたような場合にその成りすましを検出することができる。その場合、公開鍵所有者の識別情報として電子指紋を用いた場合には検証が極めて簡易になる。

【００８２】イメージ画面には、広告以外に公開鍵所有者の意向により、図７（ｃ）に示したような好みの画面、あるいは図７（ｄ）に示したように本人の写真を使用することが可能である。これらの場合は、掲載料を徴収して放送費用に充当することができる。

【００８３】なお、この実施例で埋め込まれる不可視の電子透かしは公開鍵管理センタのみが確認することができるようにされているが、確認だけはユーザができるようにすることもできる。その場合、公開鍵所有者識別情報として電子指紋を用い、ユーザが公開鍵所有者に電子指紋を確認するようにすることもできる。

【００８４】図８により、公開鍵がユーザの要求に応じて配布される本発明の他の実施例を説明する。図６に関して説明した放送により公開鍵を配布するデジタルコンテンツ管理システムは、主として電子商取引等不特定多数のユーザに公開鍵を配布する場合に有効なシステムである。これに対して、個人的なメールを送付する場合には公開鍵を配布する相手は特定少数であることが多く、

放送によって配布する必要はない。図８に示されたデジタルコンテンツ管理システムでは、公開鍵はネットワークを経由して個別に配送されるため、電子メイル等における公開鍵認証方式で採用されるＰＧＰ(Pretty Good Privacy)方式に代わる簡易認証方式として用いることができる。

【００８５】この図において、３１は公開鍵所有者、３２は公開鍵管理センタ、３３はネットワーク、３４はユーザである。ネットワーク３３は公衆通信回線あるいは双方向性ＣＡＴＶ回線であり、公開鍵所有者３１とユーザ３４との間及び公開鍵管理センタ３２とユーザ３４との間はネットワーク３３で接続されており、公開鍵所有者３１と公開鍵管理センタ３２との間は適宜な情報伝達手段により接続される。

【００８６】このように構成されたデジタルコンテンツ管理システムにおいて、公開鍵所有者３１は所有する公開鍵と公開鍵所有者識別用データとして公開鍵所有者本人であることを証明する何らかのデータをネットワーク３３を経由する経路３５により公開鍵管理センタ３２に転送する。

【００８７】公開鍵管理センタ３２は図７（ａ）に示された公開鍵配布画面の所定の位置に公開鍵を挿入するとともに公開鍵配布画面のイメージ画面に公開鍵所有者識別データを不可視電子透かしとして埋め込んで、経路３６により公開鍵所有者３１に返送する。なお、このデジタルコンテンツ管理システムにおいても使用される公開鍵所有者識別用データ及び公開鍵配布画面は、図６に示されたデジタルコンテンツ管理システムの場合と同一であるため、ここでの再度の説明は省略する。

【００８８】公開鍵所有者３１の公開鍵を入手しようとするユーザ３４はネットワーク３３を経由して経路３７により公開鍵所有者３１に公開鍵の配布を依頼し、この依頼に応じて公開鍵所有者３１はネットワーク３３を経由する経路３８により公開鍵配布画面をユーザ３４に転送する。

【００８９】ユーザ３４は転送された公開鍵配布画面から公開鍵を分離し、分離された公開鍵を用いて電子メールを暗号化し、公開鍵所有者３１に送信する。公開鍵所有者３１は、暗号化メールを所有する専用鍵を用いて復号する。

【００９０】ユーザ３４が、転送された公開鍵の真偽に疑いを持った場合には経路３９により転送された公開鍵配布画面を公開鍵管理センタ３２に転送する。公開鍵管理センタ３２は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、その結果を経路４０によりユーザ３４に通知する。このようにすることにより、他人が公開鍵所有者３１に成りすましていたような場合にその成りすましを検出することができる。

【００９１】この実施例では、公開鍵配布画面を公開鍵所有者３１がユーザ３４に直接に配布しているが、この他に公開鍵配布画面を公開鍵管理センタ３２が管理し、配布するように構成することもできる。

【００９２】図９及び図１０により、公開鍵がユーザの要求に応じて配布される本発明のさらに他の実施例を説明する。この実施例では、電子商取引用の公開鍵を取り扱う。図６に示された実施例及び図８に示された実施例では、電子透かしを用いて公開鍵所有者の検証を行っているが、図９及び図１０に示された実施例では、公開鍵使用者の検証を行う。

【００９３】図９に示されたデジタルコンテンツ管理システムにおいて、４１は公開鍵所有者、４２は公開鍵管理センタ、４３はネットワーク、４４はユーザである。ネットワーク４３は公衆通信回線あるいは双方向性ＣＡＴＶ回線であり、公開鍵所有者４１とユーザ４４との間、公開鍵所有者４１と公開鍵管理センタ４２との間、ユーザ４４と公開鍵管理センタ４２との間はネットワーク４３により各々接続される。

【００９４】このように構成されたデジタルコンテンツ管理システムにおいて、初めに公開鍵所有者４１は所有する公開鍵を経路４５により公開鍵管理センタ４２に転送し、公開鍵管理センタ４２は転送された公開鍵を保管している。公開鍵所有者４１に対して電子商取引で発注等の行為を行おうとするユーザ４４は、ユーザ４４の身元を証明する何らかのユーザ識別データをネットワーク４３を経由する経路４６により公開鍵管理センタ４２に転送する。

【００９５】公開鍵管理センタ４２は図１０（ａ）に示された公開鍵配布画面の所定の公開鍵挿入位置に公開鍵を挿入するとともに図１０（ｂ）に示されたように公開鍵配布画面のイメージ画面にユーザ４４の識別データを不可視の電子透かしとして埋め込んで、ネットワーク４３を経由する経路４７によりユーザ４４に転送する。

【００９６】ここで使用するユーザ識別用データとして、ユーザ名等の情報を直接に利用することも可能であるが、その情報をＭＤ５ハッシュアルゴリズムによって１６バイトのデータに縮小した電子指紋を利用することができる。

【００９７】公開鍵配布画面は挿入された公開鍵を容易に分離することができるようにＨＴＭＬ形式あるいはＸＭＬ形式を使用して作成されており、その一部にはイメージデータが挿入されている。このイメージデータには、ユーザ４４の識別データ(USER'S ID) が不可視の電子透かしとして埋め込まれている。この不可視の電子透かしのアルゴリズム及び埋め込み位置は公開鍵管理センタのみが知っており、公開鍵管理センタが確認する場合には図１０（ｂ）にように内容を知ることができるが、その他の者が見た場合には図１０（ａ）のような通常の画面であり、電子透かしの内容を知ることはできない。

【００９８】このイメージ画面は広告にしておけば公開

鍵配布に要する経費を広告料によって賄うことができる。また、その他の部分には緊急情報・告知情報等の付加情報を掲載することができる。さらに、有効期間を設ける等の管理を行うためにタイムスタンプを付加してもよい。このイメージデータは写真を利用することが最適であるが、音声データが利用可能な場合には利用される音声データに電子透かしを埋め込むことも可能である。

【００９９】ユーザ４４は転送された公開鍵配布画面から公開鍵を分離し、分離された公開鍵を用いて発注書を暗号化し、転送された公開鍵配布画面とともに公開鍵所有者４１に送信する。公開鍵所有者４１は、暗号化発注書を所有する専用鍵を用いて復号し、受注業務を行う。

【０１００】公開鍵所有者４１が発注者の真偽に疑いを持った場合には、ネットワーク４３を経由する経路４８により送信された公開鍵配布画面を公開鍵管理センタ４２に転送する。公開鍵管理センタ４２は、転送された公開鍵配布画面のイメージ画面に埋め込まれた不可視電子透かしを検証し、その結果を経路４９により公開鍵所有者４１に通知する。このようにすることにより、ユーザ４４に他人が成りすましていたような場合に、その成りすましを検出することができる。

【０１０１】イメージ画面には、広告以外に公開鍵所有者の意向により、図１０（ｃ）に示したような好みの画面、あるいは図１０（ｄ）に示したように本人の写真を使用することが可能である。これらの場合は、掲載料を徴収して放送費用に充当することができる。

【図面の簡単な説明】

【図１】本発明で使用されるデジタルコンテンツ管理機能付きオペレーティングシステムの構成概念図。

【図２】デジタルコンテンツの不正利用監視を行う本発明のデジタルデータ管理システムの構成図。

【図３】本発明のデジタルデータ管理システムによる管理状態の説明図。

【図４】本発明のデジタルデータ管理システムによる他の管理状態の説明図。

【図５】　デジタルコンテンツの不正利用監視を行う本発明の他のデジタルデータ管理システムの構成図。

【図６】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明のデジタルデータ管理システムの構成図。

【図７】図６のデジタルデータ管理システムによる公開鍵を配布する方法の説明図。

【図８】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明の他のデジタルデータ管理システムの構成図。

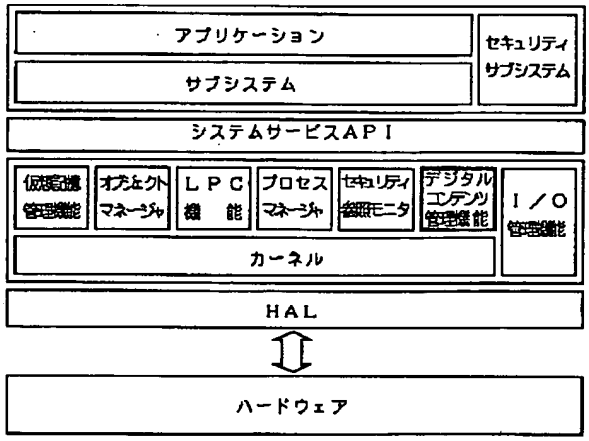
【図９】デジタルコンテンツの管理を行うために使用する公開鍵を配布する本発明のさらに他のデジタルデータ管理システムの構成図。

【図１０】図９のデジタルデータ管理システムによる公開鍵を配布する方法の説明図。

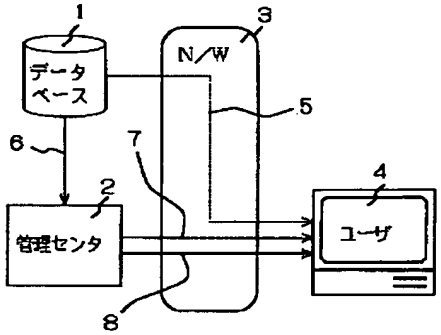
【符号の説明】

１　データベース
２　デジタルコンテンツ管理センタ
３，１３，２４，３３，４３　ネットワーク
４，１４，２５，３４，４４　ユーザ
１１　データベース
１２　デジタルコンテンツ管理センタ
１９，２３　放送局
２１，３１，４１　公開鍵所有者
２２，３２，４２　公開鍵管理センタ

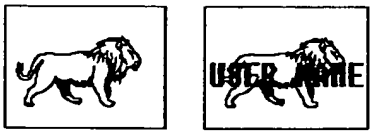
【図１】



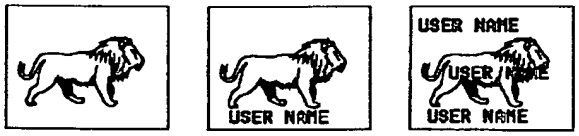
【図２】



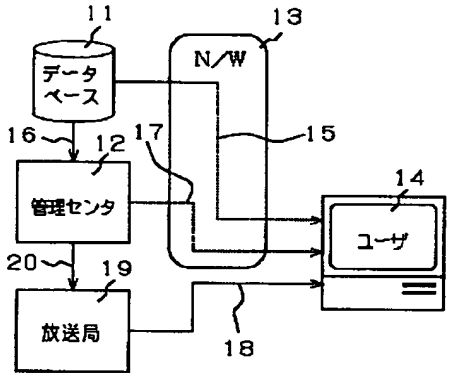
【図３】



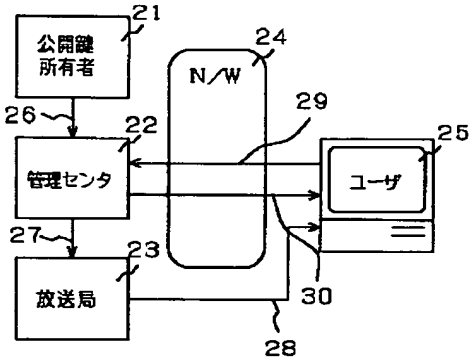
【図４】



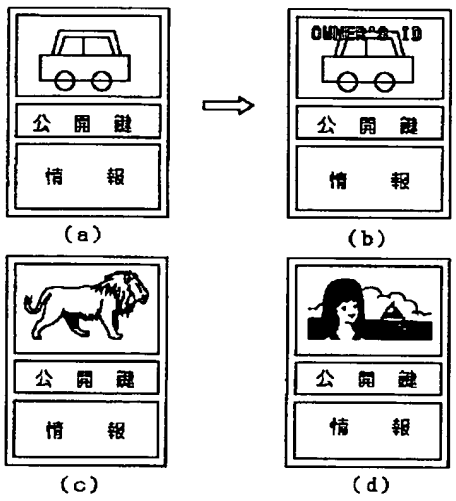
【図５】



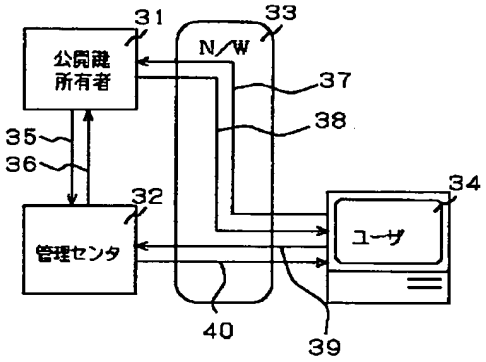
【図６】



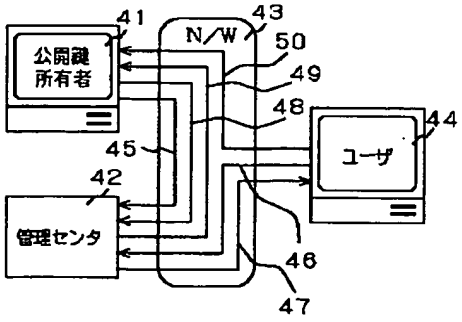
【図７】



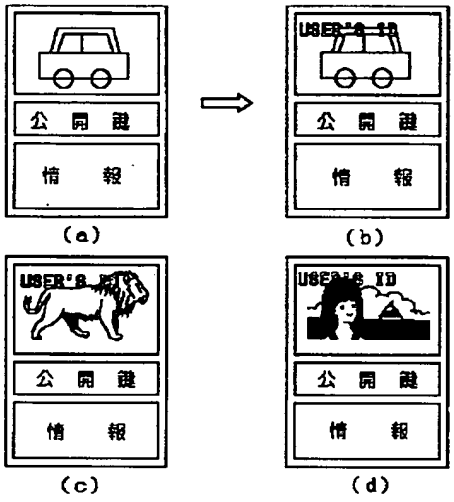
【図８】



【図９】



【図１０】



PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-007241

(43)Date of publication of application : 12.01.1999

---

(51)Int.Cl. G09C 5/00

G06F 12/14

G09C 1/00

H04N 7/08

H04N 7/081

---

(21)Application number : 09-173168 (71)Applicant : MITSUBISHI CORP

(22)Date of filing : 13.06.1997 (72)Inventor : SAITO MAKOTO

---

(54) DIGITAL CONTENTS CONTROL SYSTEM USING ELECTRONIC WATERMARK

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent an unjust use on a user side device in the protection of the copy-right of digital contents by operating a use monitoring program as a process with priority higher than a digital contents control program. SOLUTION: A data base 1 transfers ciphered digital contents to a user 4 through a network 3. Further, it transfers a cipher key for deciphering/ deciphering the ciphered digital contents to a digital contents control center 2. The control center 2 ciphers the cipher key to transmit it to the user 4. Further, the control center 2 transmits a monitoring program to the user 4. The digital contents control program incorporated in a device used by the user 4 controls the preservation/copy/transfer of the digital contents. The monitoring program interrupting into the control program detects that the preservation/copy/transfer being an irregular use are performed and embeds a visible electronic watermark

in the original digital contents.

LEGAL STATUS [Date of request for examination] 14.06.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

JPO and INPIT are not responsible for any

damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] the digital content managerial system which manages the digital content by which the copyright opinion was made -- it is -- : -- a digital content manager incorporates said digital content managerial system as a microkernel into the operating system of a user's equipment -- having -- **** --; -- said digital content manager and the use supervisor to link transmit to said user equipment by broadcast -- having --; -- said use supervisor supervises the use situation of said digital content as a process that interrupt priority is higher than said digital content manager.

[Claim 2] The digital content managerial system according to claim 1 which embeds said user's information as a visible watermark at said digital content when unjust use is detected as said use situation.

[Claim 3] The digital content managerial system according to claim 1 which embeds said user's information as an invisible watermark at said digital content

when unjust use is detected as said use situation.

[Claim 4] The digital content managerial system according to claim 1 which embeds said user's information as an invisible watermark at said digital content when preservation and a copy, and/or a transfer are ******(ed) as said use situation.

[Claim 5] It is the digital content managerial system with which a public key management center delivers a public key to a user. The :aforementioned digital content managerial system Said public key is entered in a public key distribution screen, and is distributed by broadcast, and image information is attached to the; aforementioned public key distribution screen. The information of the owner of said public key to the; aforementioned image information as invisible digital watermarking If it is embedded, the; aforementioned user separates and uses said public key from said public key distribution screen and the; aforementioned user shows said public key management center said public key distribution screen, said public key management center will check a public key owner by said invisible digital watermarking.

[Claim 6] The digital content managerial system according to claim 5 with which the electronic fingerprint of the information of the owner of said public key is used as information of the owner of said public key.

[Claim 7] It is the digital content managerial system with which a public key

management center delivers a public key to a user. The :aforementioned digital content managerial system Said user demands distribution of said public key of said public key management center, and the; aforementioned public key management center enters said public key in a public key distribution screen. Said user is supplied widely and image information is attached to the; aforementioned public key distribution screen. The information of the owner of said public key to the; aforementioned image information as invisible digital watermarking If it is embedded, the; aforementioned user separates and uses said public key from said public key distribution screen and the; aforementioned user shows said public key management center said public key distribution screen, said public key management center will check the owner of said public key by said invisible digital watermarking.

[Claim 8] The digital content managerial system according to claim 7 with which it replaces with the information of the owner of said public key, and the electronic fingerprint of the information of the owner of said public key is used.

[Claim 9] It is the digital content managerial system with which a public key management center delivers a public key to a user. The :aforementioned digital content managerial system Said user shows said public key management center said user's information. Require distribution of said public key and the; aforementioned public key management center enters said public key in a public

key distribution screen. Supply said user widely, image information is attached to the; aforementioned public key distribution screen, said user's information is embedded as invisible digital watermarking at the; aforementioned image information, and the; aforementioned user separates said public key from said public key distribution screen. With the digital content enciphered using said public key If said public key distribution screen is transmitted to the owner of said public key and the owner of the; aforementioned public key shows said public key management center said public key distribution screen, said public key management center will check said user by said invisible digital watermarking.

[Claim 10] The digital content managerial system according to claim 9 with which it replaces with said user and the electronic fingerprint of said user's information is used.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Application of the Invention] This invention relates to the system which performs management of a digital content especially copyright management of the digital

content to which the copyright opinion was carried out, and security of a digital content.

[0002]

[Description of the Prior Art] The database system which uses mutually various kinds of data which each computer saved independently by connecting each computer by the communication line until now today when it is called the information age is spreading. coding information with little amount of information which can process the information which set to this database system and has been treated by until by classic computer -- and it was monochrome binary data like facsimile information in ** and time at most, and amount of information like natural drawing and an animation could not be markedly alike, and was not able to deal with many data.

[0003] By the way, while the digital processing technique of various electrical signals develops, development of a digital processing technique is conventionally furthered also for picture signals other than the binary data currently treated only as an analog signal. Since it becomes possible to treat a picture signal like a television signal by computer by digitization of this picture signal, the "multi-media system" which deals with the data of the various kinds which a computer treats, and the image data which digitized the picture signal to coincidence attracts attention as a future technique.

[0004] Since quality deteriorated whenever the analog contents which have spread widely conventionally carry out preservation, a copy, processing, and a transfer, processing of the copyright produced according to these activities did not become a big problem. However, since quality degradation does not produce a digital content even if it repeats preservation, a copy, processing, and a transfer and performs them, processing of the copyright produced according to these activities is a big problem. Until now, there is no exact approach in copyright processing of a digital content, and it is the Copyright Act, or is processed by the contract, and the compensation to sound recording / image transcription device of a digital method is institutionalized also in the Copyright Act.

[0005] the directions of a database are online via a communication line about the digital content used effectively and processed by it not only referring to the contents, but saving, copying and processing the usually obtained digital content -- it is -- it is even possible to transmit to others, or to transmit to a database using a suitable storage, further off-line, and to register as new data. Although only alphabetic data had been applicable in the conventional database system, in a multi-media system, in addition to data, such as an alphabetic character put in a database until now, the voice data and the image data which are originally analog contents are digital-content-ized, and let them be a database.

[0006] In such a situation, although how the copyright of the digital content put in a database is dealt with poses a big problem, the copyright management tool for it and especially the copyright management tool completed about secondary use of a copy, processing, a transfer, etc. are not the place which is the former. In addition, although the digital content called software with an advertisement or freeware does not need dues in principle in use, copyright exists and may receive the limit on copyright depending on the method of use.

[0007] In view of such a situation, it aimed this invention person at protecting the copyright of a digital content until now, and he has performed various proposals to until. this invention persons proposed the equipment for it for the system which performs copyright management by JP,6-132916,A by an authorization key coming to hand from a key management center through a public telegraph and telephone circuit by JP,6-46419,A and JP,6-141004,A.

[0008] Moreover, in JP,7-271865,A and JP,8-185448,A, it proposed about the system which manages the copyright of a digital content. In these systems and equipment, those who wish viewing and listening of the enciphered program make a viewing-and-listening application to a management center via a communication line using a communication device, and a management center performs accounting and collects a tariff while it transmits an authorization key to this viewing-and-listening application. The receiving set into which the

viewing-and-listening candidate who received the authorization key sent the authorization key into the receiving set with online or an off-line means, and the authorization key was sent cancels the code of the program enciphered with the authorization key.

[0009] In order to manage copyright in the display (voice-ization is included) of the digital content in database system also including real-time transmission of digital image contents, preservation, a copy, processing, and a transfer, the program and copyright information for managing the copyright other than the key which permits use are used for the system indicated by JP,7-271865,A. This copyright manager manages by supervising so that use which applies or is contrary to the contents of authorization may not be performed.

[0010] Moreover, this JP,7-271865,A is supplied from a database, where a digital content is enciphered, and it is decrypted by the copyright manager only at the time of a display and processing, and performing preservation, a copy, and a transfer in the condition of having been enciphered again is indicated. Furthermore, the copyright manager itself is enciphered, a copyright manager is decrypted with an authorization key, and when that the decrypted copyright manager performs a decryption and encryption of copyright data, preservation of data, and use other than a display are performed, adding copyright information including the information about an operator to original copyright information, and

saving as hysteresis is also indicated.

[0011] The deposition system of the decode / equipment for re-encryption, and the cryptographic key which have the gestalt of the board for performing copyright management in JP,8-287014,A to which this application relates, a PCMCIA card, or an IC card was proposed. Moreover, in this application, reference was made also about the television meeting of a copyright management method, and the application to electronic commerce.

[0012] The system which performs protection of the original data copyright of the processing data which used two or more data in JP,8-272745,A, and processing data copyright by checking the justification of an application by the digital signature to a processing program combining a private key method and a public key system was proposed.

[0013] In JP,8-288940,A, various gestalten for applying a copyright managerial system to a database, a video-on-demand (VOD) system, or electronic commerce were proposed.

[0014] It set to JP,8-329011,A and the system which performs the protection of copyrights of the original data in the case of using and processing two or more data and new data using the third cryptographic key and copyright label was proposed.

[0015] Management of data copyright is realized by performing a limit of

encryption / decryption / re-encryption, and the contents of use by the copyright manager so that I may be understood from the data copyright managerial system and data copyright management equipment which this invention person who explained above has proposed. This code technique and a use limit are realized by using a computer.

[0016] Furthermore, when exchanging confidential information via a network, informational encryption is performed for theft prevention. Preventing the information theft at the time of transmission by encryption is stated to USP 5504818 and 5515441, using two or more cryptographic keys in that case is stated to USP 5504816, 5353351, 5475757, and 5381480, and performing re-encryption is stated to USP5479514.

[0017] In order to use a computer efficiently, the operating system (OS) which generalizes actuation of the whole computer is used. The conventional operating system currently used with the personal computer etc. consisted of a kernel (Kernel) treating fundamental service called memory management, task management, interruption, and interprocess communication, and operating system service treating other services.

[0018] However, with the improvement in capacity of a microprocessor, the situation change by the side of a computer called the fall of the RAM price used as main storage, and improvement in the military requirement from the user to a

computer, also in the operating system which generalizes actuation of the whole computer, the improvement in functional was required and the scale of an operating system has got fat as compared with before.

[0019] In order for the operating system itself to occupy the big tooth space of the hard disk which is the preservation location, the situation where the tooth space where the application program or data which a user needs is saved becomes needy, and the user-friendliness of a computer worsens generates such an enlarged operating system.

[0020] The environmental subsystem with which the newest operating system performs the emulation of other operating systems, and screen drawing from a kernel in order to cope with such a situation, It removes as a subsystem (Sub system) which is the part which depends on a user for central subsystems, such as a security subsystem. HAL which absorbs the difference of hardware (Hardware abstraction Layer), Fundamental parts, such as a scheduling function, an interruption function, and an I/O function manager, are made into a microkernel (Micro kernel). System service API (Application Programming Interface) is made to intervene between a subsystem and a microkernel, and the operating system is constituted.

[0021] While the expandability of the operating system by functional modification or addition improves by doing in this way, the transplantation corresponding to

an application becomes easy. Moreover, it becomes easy to realize a distributed operating system by distributing to two or more computers which had the element of a microkernel connected by network.

[0022] In addition to the personal computer represented by a desktop mold or the note type, the computer is used for computer-related peripherals, various control units, a transmitter, etc. In that case, unlike the general-purpose operating system for personal computers with which a man machine interface is thought as important as a specialized operating system for en BEDDEDDO (inclusion) which suits each equipment, the real time operating system with which the earliness of activation is thought as important is adopted.

[0023] The development costs of the operating system of different dedication for every equipment incorporated as a matter of course are large. Therefore, recently, when diverting the general-purpose operating system for personal computers to some other purpose as a real time operating system for embeded (inclusion) one is proposed and it arranges the program of the proper for embeded one to the subsystem combined with a microkernel, obtaining the real time operating system for inclusion is performed.

[0024] Task management, such as scheduling and interruption processing, occurs as a big function of an operating system. There are a single task method which roughly divides into an operating system and performs only one tasking to

coincidence, and multitasking which performs two or more tasking to coincidence about task management, and multitasking is classified into multitasking depending on the task by which the change of a task is processed further, and multitasking independent of the task processed.

[0025] Although MPU cannot be released until a single task method assigns one process to MPU and the process is completed in these, a non-preemptive-multitasking method can carry out time sharing of the MPU and it can assign multiple processes, unless the process under activation returns control to an operating system, other processes are not performed, and a preemptive multitasking method interrupts the process under activation with a certain time interval, and moves control to other processes compulsorily. Therefore, only in the case of a preemptive method, the multitasking of real time is possible.

[0026] Task management in a computer is performed based on the process which is a unit with system resources, such as memory and a file, and management of a process is performed based on the thread which is the unit which assigns the CPU time which subdivided the process. In addition, a system resource will be shared in this case by all the threads within the same process, therefore one or more threads which share a system resource will exist in one process.

[0027] There is priority (Priority Spectrum) in each task processed by multitasking, and, generally it is divided into the phase of 32. In this case, the usual task which does not interrupt is classified into the dynamic class (Dynamic Classes) divided into zero to 15 steps, and the task which interrupts is classified into the real-time class (Real-Time Classes) divided into 16 to 31 steps. Interruption processing is performed considering the time amount (usually 10ms) which is called a time slice and which can be interrupted as a unit, and the usual interruption is performed by the time slice for 10ms. In such a situation, although the time slice whose time amount which is called a real-time slice recently, and which can be interrupted is 100 microseconds was proposed, if this real-time slice is used, priority can be given over the conventional interruption for 10ms, and it can interrupt.

[0028] Although a code technique is a means for making unjust use of data contents impossible, since there is no guarantee that the actuation is perfect, it cannot deny the possibility of unjust use completely. On the other hand, although a digital-watermarking technique cannot make unjust use impossible, when unjust use is discovered It is a means although it can decide that it is unjust use by verifying the contents of digital watermarking. Although there are various approaches, it is generally introduced to the Nikkei electronics No. 683 and p.99-124 "for "digital-watermarking" to keep multimedia age" (1997/2/24, Nikkei

Business Publications Co. **). Moreover, No. 684 besides this number, p.149-162, and the Walter vendor "the data hiding technique (above) supporting digital watermarking", p.155-168, "the data hiding technique supporting digital watermarking (below)" () [IBM System] It is introduced also to reproduction from Journal, vol.35, and nos.3 &4 (International Business Machines Corporation). This digital-watermarking technique is stated also to EP649074.

[0029]

[Summary of the Invention] In this application, the system which delivers the public key used for management of the system and digital content which manage the digital content to which management, especially the copyright opinion of a digital content were carried out is proposed.

[0030] In the digital content managerial system proposed with this application, unjust use of the digital content to which the copyright opinion was carried out using a network or data broadcasting is supervised. It includes in the operating system of user equipment by making a digital content manager into a microkernel, and use of the digital content to which the copyright opinion was carried out is managed by this digital content manager.

[0031] User equipment is put under management of a use supervisor and the digital content manager to link, and a use supervisor operates as a process that interrupt priority is higher than a digital content manager. This use supervisor

performs embedding of visible digital watermarking to a halt, warning, or the digital content of use, when unjust use of the digital content to which the copyright opinion was carried out is supervised and unjust use is performed. Moreover, in order to pursue a use situation also in normal use, it can replace with visible digital watermarking and invisible digital watermarking can be embedded.

[0032] Furthermore, with this application, the system which distributes a public key by the network or broadcast is proposed. Although a public key is entered in a public key distribution screen and distributed, the image information where a public key owner's information was embedded as invisible digital watermarking is attached to the public key distribution screen. If a user shows a public key management center a public key distribution screen, a public key management center will check a public key owner's justification by invisible digital watermarking.

[0033] When distributing a public key by the network, the justification of a public key or a user's justification can be checked by embedding the information of the user who charged a public key owner's information or public key as invisible digital watermarking, and checking embedded invisible digital watermarking. In that case, a check will become easy if the electronic fingerprint of a user's public key is used as a user's information.

[0034]

[Example] The example of the invention in this application is explained using a drawing. It is the biggest technical problem how unjust use with user side equipment is prevented in the protection of copyrights of a digital content, and decode / re-code, and a use limit are performed by the digital content manager for the purpose of this in the "database copyright management method" of JP,7-271865,A. since [however,], as for the digital content which is the object of protection of copyrights, decode / re-code is performed by user side equipment -- processing of decode / re-code -- and -- therefore, it is hard to expect that management of the cryptographic key used is thoroughgoing, and a digital content may be unjustly saved, copied, transmitted and processed by cancelling a digital content manager.

[0035] In order to restrict such unjust use, a user needs to take care not to change the digital content manager which performs decode / re-cipher processing of a digital content, and management of a cryptographic key, and, for that purpose, it is an approach with the most positive hardware(firmware)-izing of a digital content manager. For example, there is a configuration carried out as [be / decode / re-cipher processing of a digital content, and management of a cryptographic key / possible] only by using the digital content management equipment of dedication like the scramble decoder of the dedication currently

used for descrambling of the program scrambled in current analog television broadcasting.

[0036] Although such a configuration is trustworthy, when the system configuration lacks in flexibility and modification of user side equipment or a change of a digital content manager is made, it is serious that a user deals with these modification.

[0037] Even if it is the case where modification of user side equipment or a change of a digital content manager is made, in order to cope with it flexibly, it is desirable for a digital content manager to be software, but an alteration may be performed when a digital content manager is an application program. Therefore, in order for a digital content manager to be software, it is necessary to include a digital content manager in the kernel which is the fixed area of the operating system (OS) with which a user cannot change.

[0038] However, it is not realistic when a digital content manager is included in a fixed area called a kernel, and the digital content managerial system and the code system change with databases.

[0039] When the use situation of a digital content with a copyright opinion be supervise and unjust use be discover , without affect the whole actuation by there be a thing in which interruption actuation be possible in a real time operating system by real-time slice time amount earlier figures double [1-] than

the time slice time amount of the system in other operating systems also including a kernel field , and use this technique as state above , warning or the compulsive termination of use can be carry out . Next, how to reinforce a digital content manager using a real time operating system is explained.

[0040] Since unjust use of a digital content is performed by [of the decoded digital content] unauthorized processing, unauthorized preservation, unauthorized-copying or unauthorized transmitting, the existence of unjust use is detectable with the existence of processing of a decryption digital content, preservation, a copy, or a transfer. Therefore, the process which supervises unjust use interrupts the process which a digital content manager is performing with a certain time interval, and interrupts by the multitasking of the preemptive method which supervises compulsorily.

[0041] Usually, the multitasking time slice used is 10ms, and decode / re-code process is also performed by this time basis. On the other hand, the fastest real-time slice is 1/100 of 100 microseconds. Therefore, when the use situation of the existing digital content of a copyright opinion can be supervised and unjust use is discovered, without giving effect to the just use whose user is performing whether the decoded digital content has processed, saved, copied or uploaded by interrupting and supervising by the high monitor task of priority, warning or the compulsive termination of use can be carried out.

[0042] The digital content manager which has such a monitoring function is included in the subsystem field which operates by not a kernel part but the user mode of an operating system, and a monitor process is made into the high process of priority.

[0043] By this configuration, the monitor of the existence of use of the digital content in decode / re-code and the unjust use besides authorization can be performed that it is simultaneous and smoothly.

[0044] The configuration of the operating system with which the digital content manager was included in drawing 1 is shown. This operating system consists of a subsystem which operates by the Management Department (Executive) which operates by the kernel mode which a user cannot operate, and the user mode which a user can operate, the Management Department and a subsystem have interfaced by system service API (Application Programming Interface), and HAL (Hardware abstraction Layer) intervenes between hardware and the kernel section.

[0045] The subsystem consists of a central subsystem and application programs, such as an environmental subsystem which performs the emulation of other operating systems, and screen drawing, and a security subsystem.

[0046] The virtual-memory-management function which is a microkernel (micro kernel) at the Management Department (virtual memory manager), An object

manager, an LPC (Local Procedure Call) function, a process manager, and a security reference monitor, To the I/O function manager (I/O manager) which manages the I/O between the kernels, disks, and networks which are the most fundamental element The digital content manager which manages the digital content to which the copyright opinion was furthermore carried out, Namely, the digital content function manager (digital content manager) is incorporated. Management of the preservation which is an important part in management of a digital content, a copy, or a transfer is performed when a digital content function manager manages an I/O function manager.

[0047] The example of the digital content managerial system with which the invention in this application is applied was shown in drawing 2 . In this digital content managerial system, the monitor of the digital content use situation by the user is performed through a network. In this drawing, as for a database and 2, 1 is [a digital content management center and 4] users, and the user 4, the database 1, and the digital content management center 2 are connected in the network 3 which is a public communication channel or a bidirection CATV circuit.

[0048] The digital content is accumulated in the database 1 and an encryption digital content is transmitted to a user 4 via the path 5 shown with the broken line. A database 1 transmits the cryptographic key for decode for carrying out the decode / re-code of the encryption digital content, and the cryptographic key for

re-codes to the digital content management center 2 according to a path 6, and the digital content management center 2 enciphers the cryptographic key for decode and the cryptographic key for re-codes which were transmitted, and it delivers it to a user 4 via the path shown with the broken line 7. Moreover, the digital content management center 2 transmits a supervisor to a user 4 in the path 8 shown as the continuous line.

[0049] Although the contents of use authorization are managed by the digital content manager included in the equipment which a user 4 uses, possibility that use out of range which the digital content manager has managed will be performed by the malicious user cannot be denied completely. The digital content manager has managed I/O of a user's 4 equipment, and all I/O from the memory in a user, i.e., preservation, a copy, and a transfer, is managed by the digital content manager, and when a digital content is saved, copied and transmitted, they are re-enciphered. However, it is detected by the supervisor which interrupts a digital content manager that preservation, the copy, and the transfer of a digital content should be performed by the malicious user even when it can be made not to perform this management.

[0050] Monitor actuation is performed by linking a supervisor with the digital content manager included in the equipment which a user 4 uses, and interrupting processing of a digital content manager. It supervises whether the

user is performing use beyond the contents of use authorization. The supervisor which detected that the preservation, the copy, and the transfer which is such irregular use were performed is replaced with the display of warning shown in JP,7-271865,A. Embedding of visible digital watermarking shown in drawing 3 (b) to the original digital content shown in the compulsive re-encryption or drawing 3 (a) by the cryptographic key in which a halt of decode processing and a user do not have a concern, or embedding to the digital content of invisible digital watermarking shown in drawing 4 (b) is performed.

[0051] The contents of use authorization point out the preservation to simple use of a digital content, and built-in storage, the copy to an external medium, and the transfer to other users who go via a network here. in addition, being embedded as visible digital watermarking -- discernment, such as a user's identifier, -- an easy thing is suitable.

[0052] The supervisor has collaborated during actuation of the digital content manager built in user equipment. If it has not collaborated with a supervisor, he is trying in other words for a digital content manager not to operate. For that purpose, if it makes for the supervisor to have started via a network into the conditions for starting a digital content manager or a digital content manager is started, he is trying to be automatically started in a supervisor via a network. When a user uses the digital content transmitted to a user via a network, it mixes

in the digital content transmitted and a supervisor is also transmitted.

[0053] In addition, a supervisor is united with a digital content manager, the monitor command which makes monitor actuation perform to a digital content manager is transmitted, and monitor actuation can be made to perform to a digital content manager.

[0054] In the digital content managerial system performed through a network, in treating a digital content with much amount of information, such as image data, it uses an ISDN (Integrated System for Digital Network) circuit as a communication line in many cases. Although, as for a digital content, the control channel whose data transmission rates to which the DCH whose data transmission rates to which what is generally used as this ISDN circuit is called B channels are 64Kbps(es) is called two channels and D channel are 16Kbps(es) is transmitted by the DCH of 1-2 channels as those with one channel, and a matter of course, D channel is not used in many cases. then -- if it is made like [performing the interruption monitor by the supervisor by this D channel] -- use of a digital content -- completely -- effect ****** -- there are nothings and it becomes possible to perform the remote monitor of a use situation.

[0055] Moreover, when using a public communication channel, the interruption monitor by the supervisor can be efficiently performed by using for download the ADSL (asymmetric digital subscriber line) technique in which the data

transmission rate of a maximum of 56 Kbps is realizable.

[0056] What is shown in drawing 4 is an example which embeds digital watermarking, even if it is the case of preservation, copy, and transfer of the normal contained in the contents of use authorization. Digital watermarking in this case is invisible digital watermarking detected by the digital-watermarking detection means as shown in (b), and when not based on a digital-watermarking detection means, as shown in (a), there is instead of [no] apparently with a original digital content. in addition, being embedded like the case of visible digital watermarking -- discernment, such as a user's identifier, -- an easy thing is suitable.

[0057] By doing in this way, even if it is normal use in the beginning, when unjust use is performed later, the path of preservation, a copy, and a transfer can be checked. Moreover, even if it is the thing of normal, by repeating preservation, a copy, and a transfer, as shown in (c), invisible digital watermarking increases, and, as a result, the quality of a digital content deteriorates. According to such a thing, it is lost that preservation, a copy, and a transfer are repeated by infinity, and management of a digital content becomes easy.

[0058] "Re-encryption" which is an element important for digital content management is the process that a burden is quite heavy for a user's equipment. Therefore, it is also effective in preventing unjust use of a digital content to

embed digital watermarking as a short form.

[0059] In charging the meter ring data whose digital content management center is a use track record by polling recovering later although accounting is performed easily if a user is made for a use authorization key to come to hand beforehand as shown in JP,7-271865,A when use of a digital content is performed for pay, it puts meter ring data under management of a user until polling is performed. Therefore, the alteration of meter ring data is performed by the malicious user, and it is possible that normal accounting is barred.

[0060] When the user uses the digital content in the digital content managerial system of this example, user equipment is always connected to a management center, and the monitor of the use situation by the supervisor is performed. Therefore, by keeping meter ring data in the digital content management center in this monitor actuation, the need for polling is lost and the alteration of the meter ring data by the user can be prevented. Moreover, even if it is the case where use of a digital content is performed for nothing, the use situation by the user can be grasped easily.

[0061] The block diagram of other examples of the digital content managerial system with which the invention in this application is applied was shown in drawing 5 . The monitor of a digital content use situation is performed by broadcast in this digital content managerial system. In this drawing, as for a

database and 12, 11 is [a digital content management center and 14] users, and the user 14, the database 1, and the digital content management center 12 are connected in the network 13 which is a public communication channel or a bidirection CATV circuit.

[0062] The digital content is accumulated in the database 11 and an encryption digital content is transmitted to a user 14 via the path 15 shown with the broken line. The digital content management center 12 enciphers the cryptographic key for decode for carrying out the decode / re-code of the encryption digital content, and the cryptographic key for re-codes, and delivers them to a user 14 via the path shown with the broken line 17. Moreover, the digital content management center 12 transmits a monitor command to a broadcasting station 19, and a broadcasting station 19 transmits the transmitted monitor command to a user 14 in the path 18 shown as the continuous line.

[0063] Although this path 18 has the most common broadcasting electric-wave, the CATV cable which is wire broadcasting is also available, and it is also possible to use a network when Internet broadcast is performed further.

[0064] Invisible digital watermarking shown in visible digital watermarking which this monitor command interrupts the actuation which the digital content manager included in the equipment which a user 14 uses is performing, and the user made the digital content manager supervise whether use beyond the contents of

use authorization is carried out, was made to suspend decode processing when preservation, a copy, and a transfer were performed, or was shown in drawing 3 , or drawing 4 is embedded to a digital content.

[0065] The monitor command is performing interruption actuation during actuation of the digital content manager built in user equipment. If the broadcast wave it is broadcast that a monitor command is is not received, he is trying in other words for a digital content manager not to operate. For that purpose, if it makes to have received the monitor command via a broadcast wave into the conditions for starting a digital content manager or a digital content manager is started, the monitor command which goes via a broadcast wave automatically will be received. When a user uses the digital content transmitted to a user by data broadcasting etc., it mixes in the digital content transmitted and a monitor command is also transmitted.

[0066] The digital content manager has managed I/O of a user's 14 equipment, and all I/O from the memory in a user, i.e., preservation, a copy, and a transfer, is managed by the digital content manager, and when a digital content is saved, copied and transmitted, they are re-enciphered. It is detected by the supervisor which interrupts a digital content manager that preservation, the copy, and the transfer of a digital content should be performed by the malicious user even when it can be made not to perform this management.

[0067] The supervisor which detected that such irregular use was performed is replaced with the display of warning shown in JP,7-271865,A, and embedding of visible digital watermarking as shown in drawing 3 (b) is performed. Moreover, even if it is the case of preservation, copy, and transfer of the normal contained in the contents of use authorization, it is also possible to embed invisible digital watermarking which will not be detected without a digital-watermarking detection means as shown in drawing 4 (b) and (c).

[0068] A user does not perform monitor actuation through these broadcasts or networks of a user's volition, but when using the digital content to which the copyright opinion was carried out, it is automatically carried out by the digital content manager. In order to ensure this actuation furthermore, when monitor actuation through broadcast or a network is not performed, it is made not to be carried out in actuation of the decode/encryption by the digital content manager. Moreover, when using the digital content to which the copyright opinion was carried out, it connects with the management center which transmits the reception or the supervisor of an electric wave which broadcasts a supervisor automatically.

[0069] Next, the example which distributes a public key is explained. What has the large cryptographic key for which what has the large magnitude of the cryptographic key used by the private key (secret key) system called a common

key (common key) system is used by the public key (public key) system to being about 100 bits exceeds 1000 bits. Since a public key system requires time and effort for encryption/decryption while safety is high, it is used for a data encryption with small sending of a private key, digital signature, and amount of authentication isochore, and encryption of a digital content is performed using a private key. in a public key system, a public key and an exclusive key (private key) are used, being put together -- having -- an exclusive key -- the bottom of management of an owner -- although he and others cannot know, the public key needs to be told to others on the purpose of use.

[0070] Therefore, although there are few possibilities that a fake public key may be distributed if a public key can be directly received from an owner in that case although a public key is distributed to the public with various means, when that is not right, a fake public key may be received. the digital content managerial system which can look like [business] the truth of the public key distributed also in the indirect distribution approach of going via broadcast or a network, in the public key in this example, and can check it -- so to speak, a key distribution network is proposed.

[0071] The example of this invention of the digital content managerial system which distributes a public key to drawing 6 by broadcast is shown. In this digital content managerial system, since it is generally delivered widely, a public key

can be used as a simple authentication method replaced with the PEM (Privacy Enhanced Mail) method adopted by the public key authentication method in electronic commerce etc.

[0072] For a public key owner and 22, as for a broadcasting station and 24, in this drawing, a public key management center and 23 are [21 / a network and 25] users. Broadcasting stations 23 are television or voice broadcasting stations, such as a terrestrial analog, a satellite analog, a CATV analog, terrestrial digital one, satellite digital, and CATV digital, and data broadcasting is performed by proper means, such as scanning-line multiplex (Vertical Blanking Interval:VBI), voice multiplex, and data mixing. In addition, the Internet broadcasting station is also available as this broadcasting station. A network 24 is a public communication channel or a bidirection CATV circuit, between the public key management center 22 and a user 25, it connects in the network 24 and a proper signal transduction medium connects between a broadcasting station 23 and a user 25.

[0073] thus, the public key which the public key owner 21 owns in the constituted digital content managerial system and a public key owner -- it transmits to the public key management center 22 according to a path 26 by using a certain data proving being him as the data for public key owner discernment. As data for public key owner discernment used here, although information, such as a public

key owner name, is used directly, the electronic fingerprint which reduced the information to 16 bytes of data by the MD5 hash algorithm can also be used.

[0074] The public key management center prepares the public key distribution screen as shown in drawing 7 (a), and inserts a public key in a position. This screen is created using the HTML (Hyper Text Markup Language) format or the XML (eXtensible Markup Language) format so that the inserted public key can be used dissociating easily, and the image data is inserted in that part.

[0075] In this image data, it is the public key owner's 21 data for discernment (OWNER'S ID). It is embedded as invisible digital watermarking. Although only the public key management center knows this invisible algorithm and invisible embedding location of digital watermarking, and the contents of digital watermarking can be known as the public key management center was shown in drawing 7 (b), when other persons see, it is a usual screen like drawing 7 (a), and the contents of digital watermarking cannot be known.

[0076] If the advertisement is carried as this image screen, the cost which public key distribution takes can be covered by the charge of advertising printing. Moreover, into other parts, additional information, such as emergency intelligence and notice information, can be carried. Furthermore, a time stump may be added in order to manage preparing a shelf-life etc. Although it is optimal to use a photograph as this image data, when voice data is available, it is also

possible to embed digital watermarking at the voice data used.

[0077] A broadcasting station 23 broadcasts the public key distribution screen created by doing in this way according to the broadcast path 28.

[0078] Although a user 25 receives the broadcast public key distribution screen, since digital watermarking embedded on the image screen of the public key distribution screen which the user 25 received is an invisible thing, a user 25 cannot know the contents of digital watermarking.

[0079] Although a user 25 separates a public key from the broadcast public key distribution screen and uses it for various electronic commerce, when it has misgiving in the truth of a public key, he transmits a public key distribution screen to the public key management center 22 according to the path 29 by the network 24.

[0080] The public key management center 22 verifies invisible digital watermarking embedded on the image screen of the transmitted public key distribution screen, and notifies a user 25 of it according to the path 30 by the network 24 about a public key owner's identification information detected as shown in drawing 7 (b).

[0081] By doing in this way, when others have become completely, the ********** can be detected. In that case, verification becomes very simple when an electronic fingerprint is used as a public key owner's identification information.

[0082] It is possible to use his photograph for an image screen by a public key owner's intention, in addition to an advertisement, as shown in a favorite screen as shown at drawing 7 (c), or drawing 7 (d). The charge of printing can be collected in these cases, and it can appropriate for broadcast costs.

[0083] In addition, although it is made for invisible digital watermarking embedded in this example to have only the public key management center checked, a user can do only a check. In that case, a user can check an electronic fingerprint to a public key owner, using an electronic fingerprint as public key owner identification information.

[0084] Other examples of this invention to which a public key is distributed by drawing 8 according to a demand of a user are explained. The digital content managerial system which distributes a public key by broadcast explained about drawing 6 is an effective system when distributing a public key mainly to many and unspecified users, such as electronic commerce. On the other hand, when sending individual mail, the partner who distributes a public key is a specific fraction in many cases, and does not need to distribute by broadcast. In the digital content managerial system shown in drawing 8 , since it is delivered according to an individual via a network, a public key can be used as a simple authentication method replaced with the PGP (Pretty Good Privacy) method adopted by the public key authentication method in an E-mail etc.

[0085] For 31, as for a public key management center and 33, in this drawing, a public key owner and 32 are [a network and 34] users. A network 33 is a public communication channel or a bidirection CATV circuit, and between the public key owner 31 and a user 34 and between the public key management center 32 and a user 34, it connects in the network 33 and connects with the proper means of signal transduction between the public key owner 31 and the public key management center 32.

[0086] thus -- as the public key which the public key owner 31 owns in the constituted digital content managerial system, and the data for public key owner discernment -- a public key owner -- a certain data proving being him are transmitted to the public key management center 32 according to the path 35 which goes via a network 33.

[0087] The public key management center 32 embeds public key owner discernment data as invisible digital watermarking on the image screen of a public key distribution screen while inserting a public key in the position of the public key distribution screen shown in drawing 7 (a), and it returns them to the public key owner 31 according to a path 36. In addition, since the data for public key owner discernment and the public key distribution screen which are used also in this digital content managerial system are the same as that of the case of the digital content managerial system shown in drawing 6 , explanation here for

the second time is omitted.

[0088] The user 34 who is going to receive the public key owner's 31 public key requests distribution of a public key from the public key owner 31 according to a path 37 via a network 33, and the public key owner 31 transmits a public key distribution screen to a user 34 according to the path 38 which goes via a network 33 according to this request.

[0089] A user 34 separates a public key from the transmitted public key distribution screen, enciphers an electronic mail using the separated public key, and transmits to the public key owner 31. The public key owner 31 decodes using the exclusive key which owns encrypted mail.

[0090] When a user 34 has misgiving in the truth of the transmitted public key, the public key distribution screen transmitted according to the path 39 is transmitted to the public key management center 32. The public key management center 32 verifies invisible digital watermarking embedded on the image screen of the transmitted public key distribution screen, and notifies a user 34 of the result according to a path 40. By doing in this way, when others have become the public key owner 31 completely, the ********** can be detected.

[0091] It can also constitute from this example although the public key owner 31 has distributed the public key distribution screen to the user 34 directly, in addition so that the public key management center 32 may manage and

distribute a public key distribution screen.

[0092] The example of further others of this invention to which a public key is distributed by drawing 9 and drawing 10 according to a demand of a user is explained. The public key for electronic commerce is dealt with in this example. Although the public key owner is verified using digital watermarking in the example shown in the example shown in drawing 6 , and drawing 8 , a public key user is verified in the example shown in drawing 9 and drawing 10 .

[0093] For 41, as for a public key management center and 43, in the digital content managerial system shown in drawing 9 , a public key owner and 42 are [a network and 44] users. A network 43 is a public communication channel or a bidirection CATV circuit, and a network 43 connects respectively between a user 44 and the public key management center 42 between the public key owner 41 and the public key management center 42 between the public key owner 41 and a user 44.

[0094] Thus, in the constituted digital content managerial system, first, the public key owner 41 transmits the public key to own to the public key management center 42 according to a path 45, and the public key management center 42 is keeping the transmitted public key. The user 44 who is going to perform actions, such as order, by electronic commerce to the public key owner 41 transmits a certain user-identification data proving a user's 44 identity to the public key

management center 42 according to the path 46 which goes via a network 43.

[0095] As shown in drawing 10 (b), the public key management center 42 embeds a user's 44 discernment data as invisible digital watermarking on the image screen of a public key distribution screen, while inserting a public key in the predetermined public key insertion point of the public key distribution screen shown in drawing 10 (a), and it transmits them to a user 44 according to the path 47 which goes via a network 43.

[0096] Although it is also possible to use information, such as a user name, directly as data for user identifications used here, the electronic fingerprint which reduced the information to 16 bytes of data by the MD5 hash algorithm can be used.

[0097] The public key distribution screen is created using the HTML format or the XML format so that the inserted public key can be separated easily, and the image data is inserted in the part. In this image data, it is a user's 44 discernment data (USER'S ID). It is embedded as invisible digital watermarking. Although only the public key management center knows this invisible algorithm and invisible embedding location of digital watermarking, and the contents can be known like to drawing 10 (b) when a public key management center checks, when other persons see, it is a usual screen like drawing 10 (a), and the contents of digital watermarking cannot be known.

[0098] This image screen can cover the cost which public key distribution takes by the advertising rate, if it is made the advertisement. Moreover, into other parts, additional information, such as emergency intelligence and notice information, can be carried. Furthermore, a time stump may be added in order to manage preparing a shelf-life etc. Although it is optimal to use a photograph as for this image data, when voice data is available, it is also possible to embed digital watermarking at the voice data used.

[0099] A user 44 separates a public key from the transmitted public key distribution screen, and using the separated public key, it enciphers and he transmits a purchase order to the public key owner 41 with the transmitted public key distribution screen. The public key owner 41 decodes using the exclusive key which owns an encryption purchase order, and performs order-received business.

[0100] When the public key owner 41 has misgiving in the truth of a purchaser, the public key distribution screen transmitted according to the path 48 which goes via a network 43 is transmitted to the public key management center 42. The public key management center 42 verifies invisible digital watermarking embedded on the image screen of the transmitted public key distribution screen, and notifies the public key owner 41 of the result according to a path 49. The ********** can be detected when others have become the user 44 completely by

doing in this way.

[0101] It is possible to use his photograph for an image screen by a public key owner's intention, in addition to an advertisement, as shown in a favorite screen as shown at drawing 10 (c), or drawing 10 (d). The charge of printing can be collected in these cases, and it can appropriate for broadcast costs.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The configuration conceptual diagram of the operating system with a digital content function manager used by this invention.

[Drawing 2] The block diagram of the digital data managerial system of this invention which performs the unjust use monitor of a digital content.

[Drawing 3] The explanatory view of the state of control by the digital data managerial system of this invention.

[Drawing 4] The explanatory view of other state of control by the digital data managerial system of this invention.

[Drawing 5] The block diagram of other digital data managerial systems of this invention which performs the unjust use monitor of a digital content.

[Drawing 6] The block diagram of the digital data managerial system of this invention which distributes the public key used in order to manage a digital content.

[Drawing 7] The explanatory view of the approach of distributing the public key by the digital data managerial system of drawing 6 .

[Drawing 8] The block diagram of other digital data managerial systems of this invention which distributes the public key used in order to manage a digital content.

[Drawing 9] The block diagram of the digital data managerial system of further others of this invention which distributes the public key used in order to manage a digital content.

[Drawing 10] The explanatory view of the approach of distributing the public key by the digital data managerial system of drawing 9 .

[Description of Notations]

1 Database

2 Digital Content Management Center

3, 13, 24, 33, 43 Network

4, 14, 25, 34, 44 User

11 Database

12 Digital Content Management Center

19 23 Broadcasting station

21, 31, 41 Public key owner

22, 32, 42 Public key management center